

National Cyber Alert System

[Archive](#)

Cyber Security Bulletin SB09-208

Vulnerability Summary for the Week of July 20, 2009

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities		
Primary Vendor -- Product	Description	Publish Date
activewebsoftwares -- active_web_mail	SQL injection vulnerability in Active Web Mail 4.0 allows remote attackers to execute arbitrary SQL commands via the TabOpenQuickTab1 parameter to (1) popaccounts.aspx, (2) addressbook.aspx, and (3) emails.aspx.	2009-07-23
adminnewstools -- admin_news_tools	system/message.php in Admin News Tools 2.5 does not properly restrict access, which allows remote attackers to post news messages via a direct request.	2009-07-21
adobe -- acrobat_reader nos_microsystems -- getplus_download_manager	NOS Microsystems getPlus Download Manager for Adobe 1.6.2.36, and possibly other versions, installs NOS\bin\getPlus_HelperSvc.exe with insecure permissions (Everyone:Full Control), which allows local users to gain SYSTEM privileges by replacing getPlus_HelperSvc.exe with a Trojan horse program.	2009-07-21
adobe -- acrobat	Unspecified vulnerability in Adobe Reader and Acrobat 9.x through 9.1.2 and Adobe Flash Player 9 and 10	2009-07-21

adobe -- acrobat_reader adobe -- flash_player	allows remote attackers to execute arbitrary code via (1) a crafted Flash application in a .pdf file or (2) a crafted .swf file, as exploited in the wild in July 2009.	2009-07-23
adobe -- acrobat adobe -- acrobat_reader adobe -- flash_player	Unspecified vulnerability in Adobe Reader and Acrobat 9.x through 9.1.2, and Adobe Flash Player 9.x through 9.0.159.0 and 10.x through 10.0.22.87, allows remote attackers to execute arbitrary code via (1) a crafted Flash application in a .pdf file or (2) a crafted .swf file, related to authplay.dll, as exploited in the wild in July 2009.	2009-07-23
aigo -- aigo_md_p8860	The Aigo P8860 allows remote attackers to cause a denial of service (memory consumption and browser hang) via a large integer value for the length property of a Select object, a related issue to CVE-2009-1692.	2009-07-20
akamai_technologies -- download_manager	Stack-based buffer overflow in manager.exe in Akamai Download Manager (aka DLM or dlmanager) before 2.2.4.8 allows remote web servers to execute arbitrary code via a malformed HTTP response during a Redswoosh download, a different vulnerability than CVE-2007-1891 and CVE-2007-1892.	2009-07-23
almondsoft -- almond_classifieds	SQL injection vulnerability in the Almond Classifieds (com_aclassf) component 5.6.2 for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php.	2009-07-22
aspSiteware -- autodealer	Multiple SQL injection vulnerabilities in ASP SiteWare autoDealer 1 and 2 allow remote attackers to execute arbitrary SQL commands via the iType parameter in (1) Auto1/type.asp or (2) auto2/type.asp.	2009-07-24
bistudio -- arma bistudio -- arma_2	Format string vulnerability in Armed Assault (aka ArmA) 1.14 and earlier, and 1.16 beta, and Armed Assault II 1.02 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via format string specifiers in the (1) nickname and (2) datafile fields in a join request, which is not properly handled when logging an error message.	2009-07-20
censura -- censura	SQL injection vulnerability in censura.php in Censura 1.16.04 allows remote attackers to execute arbitrary SQL commands via the itemid parameter in a details action.	2009-07-24

google -- chrome google -- v8	Heap-based buffer overflow in src/jsregexp.cc in Google V8 before 1.1.10.14, as used in Google Chrome before 2.0.172.37, allows remote attackers to execute arbitrary code in the Chrome sandbox via a crafted JavaScript regular expression.	2009-07 21
google -- chrome	Google Chrome before 2.0.172.37 allows attackers to leverage renderer access to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors that trigger excessive memory allocation.	2009-07 21
humayun_shabbir_bhutta -- asp_product_catalog	SQL injection vulnerability in default.asp in ASP Product Catalog allows remote attackers to execute arbitrary SQL commands via the cid parameter, a different vector than CVE-2007-5220.	2009-07 24
ibm -- proventia_desktop_endpoint_security ibm -- proventia_network_mail_security_system ibm -- proventia_network_mail_security_system_vitual_appliance ibm -- proventia_network_multi-function_security	Multiple unspecified vulnerabilities in the IBM Proventia engine 4.9.0.0.44 20081231, as used in IBM Proventia Network Mail Security System, Network Mail Security System Virtual Appliance, Desktop Endpoint Security, Network Multi-Function Security (MFS), and possibly other products, allow remote attackers to bypass detection of malware via a modified (1) ZIP or (2) CAB archive, a related issue to CVE-2009-1240.	2009-07 20
linux -- kernel linux -- linux_kernel	Off-by-one error in the options_write function in drivers/misc/sgi-gru/gruproofs.c in the SGI GRU driver in the Linux kernel 2.6.30.2 and earlier on ia64 and x86 platforms might allow local users to overwrite arbitrary memory locations and gain privileges via a crafted count argument, which triggers a stack-based buffer overflow.	2009-07 23
mlffat -- mlffat	SQL injection vulnerability in index.php in Mlffat 2.2 allows remote attackers to execute arbitrary SQL commands via a member cookie in an account editprofile action, a different vector than CVE-2009-1731.	2009-07 24
mozilla -- firefox mozilla -- thunderbird	The browser engine in Mozilla Firefox before 3.0.12 and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) the frame chain and synchronous events, (2) a SetMayHaveFrame assertion and nsCSSFrameConstructor::CreateFloatingLetterFrame, (3) nsCSSFrameConstructor::ConstructFrame, (4) the child list and initial reflow, (5) GetLastSpecialSibling, (6) nsFrameManager::GetPrimaryFrameFor and MathML, (7) nsFrame::GetBoxAscent, (8) nsCSSFrameConstructor::AdjustParentFrame, (9) nsDOMOfflineResourceList, and (10)	2009-07 22

	nsContentUtils::ComparePosition.	
mozilla -- firefox mozilla -- thunderbird	Integer overflow in a base64 decoding function in Mozilla Firefox before 3.0.12 and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors.	2009-07 22
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	The nsXULTemplateQueryProcessorRDF::CheckIsSeparator function in Mozilla Firefox before 3.0.12, SeaMonkey 2.0a1pre, and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to loading multiple RDF files in a XUL tree element.	2009-07 22
mozilla -- firefox mozilla -- thunderbird	Mozilla Firefox before 3.0.12 and Thunderbird allow remote attackers to cause a denial of service (memory corruption and application crash) or execute arbitrary code via vectors involving double frame construction, related to (1) nsHTMLContentSink.cpp, (2) nsXMLContentSink.cpp, and (3) nsPresShell.cpp, and the nsSubDocumentFrame::Reflow function.	2009-07 22
mozilla -- firefox mozilla -- thunderbird	The JavaScript engine in Mozilla Firefox before 3.0.12 and Thunderbird allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to (1) nsDOMClassInfo.cpp, (2) JS_HashTableRawLookup, and (3) MirrorWrappedNativeParent and js_LockGCThingRT.	2009-07 22
mozilla -- firefox	Mozilla Firefox before 3.0.12 and 3.5 before 3.5.1 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors involving a Flash object, a slow script dialog, and the unloading of the Flash plugin, which triggers attempted use of a deleted object.	2009-07 22
mozilla -- firefox	Integer overflow in CoreGraphics in Apple Mac OS X, as used in Mozilla Firefox before 3.0.12, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long text run that triggers a heap-based buffer overflow during font glyph rendering, a related issue to CVE-2009-1194.	2009-07 22
mozilla -- firefox	Mozilla Firefox before 3.0.12 does not properly handle an SVG element that has a property with a watch function and an __defineSetter__ function, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted document, related to a certain pointer misinterpretation.	2009-07 22
mozilla -- firefox	The setTimeout function in Mozilla Firefox before 3.0.12 does not properly preserve object wrapping, which allows remote attackers to execute arbitrary JavaScript with chrome privileges via a crafted call, related to XPCNativeWrapper.	2009-07 22
nokia -- n810_internet_tablet	The Nokia N95 running Symbian OS 9.2, N82, and N810 Internet Tablet allow remote attackers to cause a	2009-07 22

nokia -- n82 nokia -- symbian	denial of service (memory consumption) via a large integer value for the length property of a Select object, a related issue to CVE-2009-1692.	2009-07-20
ondanera.net -- hamster_audio_player	Stack-based buffer overflow in Hamster Audio Player 0.3a allows remote attackers to execute arbitrary code via a long string in a (1) .m3u or (2) .hpl playlist file.	2009-07-20
phpjunkyard -- gbook	SQL injection vulnerability in guestbook.php in PHPJunkYard GBook 1.6 allows remote attackers to execute arbitrary SQL commands via the mes_id parameter.	2009-07-24
pulseaudio -- pulseaudio	Race condition in PulseAudio 0.9.9, 0.9.10, and 0.9.14 allows local users to gain privileges via vectors involving creation of a hard link, related to the application setting LD_BIND_NOW to 1, and then calling execv on the target of the /proc/self/exe symlink.	2009-07-17
resalecode -- hutscripts_php_website_script	SQL injection vulnerability in showcategori.php in Hutscripts PHP Website Script allows remote attackers to execute arbitrary SQL commands via the cid parameter.	2009-07-24
rim -- blackberry_8800	The Research In Motion (RIM) BlackBerry 8800 allows remote attackers to cause a denial of service (memory consumption and browser crash) via a large integer value for the length property of a Select object, a related issue to CVE-2009-1692.	2009-07-22
runcms -- myannonces	SQL injection vulnerability in the MyAnnonces module for E-Xoopport 3.1 allows remote attackers to execute arbitrary SQL commands via the lid parameter in a viewannonces action to index.php.	2009-07-24
sony -- playstation_3	The web browser on the Sony PLAYSTATION 3 (PS3) allows remote attackers to cause a denial of service (memory consumption and console hang) via a large integer value for the length property of a Select object, a related issue to CVE-2009-1692.	2009-07-20
sorinara -- streaming_audio_player	Stack-based buffer overflow in Sorinara Streaming Audio Player (SAP) 0.9 allows remote attackers to execute arbitrary code via a long string in a playlist (.m3u) file.	2009-07-22
	Stack-based buffer overflow in the	

symantec -- wifax_pro	Symantec.FaxViewerControl.1 ActiveX control in WinFax\DCCFAXVW.DLL in Symantec WinFax Pro 10.03 allows remote attackers to execute arbitrary code via a long argument to the AppendFax method.	2009-07-22
tfm -- mmplayer	Stack-based buffer overflow in TFM MMPlayer 2.0, and possibly 2.0.0.30, allows remote attackers to execute arbitrary code via a long string in a playlist (.m3u) file.	2009-07-21
wireshark -- wireshark	Unspecified vulnerability in the Infiniband dissector in Wireshark 1.0.6 through 1.2.0, when running on unspecified platforms, allows remote attackers to cause a denial of service (crash) via unknown vectors.	2009-07-21

[Back to top](#)

Medium Vulnerabilities					
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info	
adminnewstools -- admin_news_tools	Directory traversal vulnerability in system/download.php in Admin News Tools 2.5 allows remote attackers to read arbitrary files via a .. (dot dot) in the fichier parameter.	2009-07-21	5.0	CVE-2009-2557 BUGTRAQ MILWORM SECUNIA OSVDB	
anelectron -- advanced_electron_forum	SQL injection vulnerability in Advanced Electron Forum (AEF) 1.x, when magic_quotes_gpc is disabled, allows remote attackers to execute arbitrary SQL commands via the filename in an uploaded attachment. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-07-20	6.8	CVE-2009-2545 XF SECUNIA OSVDB	
anelectron -- advanced_electron_forum	Directory traversal vulnerability in Advanced Electron Forum (AEF) 1.x allows remote attackers to determine the existence of arbitrary files via the avatargalfile parameter when changing an avatar, which leaks the existence of the file in an error message. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2009-07-20	4.3	CVE-2009-2546 XF SECUNIA OSVDB	
aspthai.net -- aspthai_forums	ASPTThai.NET ASPTThai Forums 8.5 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database via a direct request for database/aspthaiForum.mdb.	2009-07-23	5.0	CVE-2008-6872 XF VUPEN OSVDB MILWORM SECUNIA	
bioscripts -- minitwitter	Multiple SQL injection vulnerabilities in MiniTwitter 0.2 beta, when magic_quotes_gpc is disabled, allow remote authenticated users to execute arbitrary SQL commands via the (1) user parameter to (a) index.php and (b) rss.php.	2009-07-22	6.0	CVE-2009-2573 XF BID BUGTRAQ MILWORM	
	index.php in MiniTwitter 0.2 beta allows remote	2009-07		CVE-2009-2574 VUL	

bioscripts -- minitwitter	authenticated users to modify certain options of arbitrary accounts via an opt action.	2009-07-22	6.5	^F BID BUGTRAQ MILWoRM
bistudio -- arma bistudio -- arma_2	Integer underflow in Armed Assault (aka ArmA) 1.14 and earlier, and 1.16 beta, and Armed Assault II 1.02 and earlier allows remote attackers to cause a denial of service (crash) via a VoIP over Network (VON) packet to port 2305 with a negative packet_size value, which triggers a buffer over-read.	2009-07-20	5.0	CVE-2009-2547 XF VUPEN SECUNIA MISC
bistudio -- arma bistudio -- arma_2	Armed Assault (aka ArmA) 1.14 and earlier, and 1.16 beta, and Armed Assault II 1.02 and earlier allows remote attackers to cause a denial of service via a join packet with a final field whose value is (1) 0, which triggers a server crash related to memory allocation, or (2) 1, which triggers CPU/memory consumption and a NULL pointer dereference.	2009-07-20	5.0	CVE-2009-2549 VUPEN MISC
censura -- censura	Cross-site scripting (XSS) vulnerability in censura.php in Censura 1.16.04 allows remote attackers to inject arbitrary web script or HTML via the itemid parameter in a details action.	2009-07-24	4.3	CVE-2009-2594 XF BID MILWORM SECUNIA
censura -- censura	Cross-site scripting (XSS) vulnerability in productSearch.html in Censura 2.0.4 and 2.1.0 allows remote attackers to inject arbitrary web script or HTML via the q parameter in a ProductSearch action.	2009-07-24	4.3	CVE-2009-2595 XF OSVDB CONFIRM CONFIRM SECUNIA
dragdropcart -- dragdropcart	Multiple cross-site scripting (XSS) vulnerabilities in DragDropCart allow remote attackers to inject arbitrary web script or HTML via the (1) sid parameter to assets/js/ddcart.php, the (2) prefix parameter to includes/ajax/getstate.php, the search parameter to (3) index.php and (4) search.php, the (5) redirect parameter to login.php, and the (6) product parameter to productdetail.php.	2009-07-24	4.3	CVE-2009-2587 XF OSVDB OSVDB OSVDB OSVDB OSVDB SECUNIA MISC
edgephp -- ezarticles	Cross-site scripting (XSS) vulnerability in articles.php in EDGEPHP EZArticles allows remote attackers to inject arbitrary web script or HTML via the title parameter.	2009-07-24	4.3	CVE-2009-2586 XF SECUNIA MISC OSVDB
editeurscripts -- esbaseadmin	Cross-site scripting (XSS) vulnerability in default/login.php in EditeurScripts EsBaseAdmin 2.1 allows remote attackers to inject arbitrary web script or HTML via the msg parameter. NOTE: the EsContacts 1.0 issue is covered in CVE-2008-2037.	2009-07-23	4.3	CVE-2008-6868 XF BID SECUNIA MISC
editeurscripts -- esnews	Cross-site scripting (XSS) vulnerability in modifier.php in EditeurScripts EsNews 1.2 allows remote attackers to inject arbitrary web script or HTML via the msg parameter.	2009-07-23	4.3	CVE-2009-2581 XF MISC

editeurscripts -- espartenaires	Cross-site scripting (XSS) vulnerability in login.php in EsPartenaires 1.0 allows remote attackers to inject arbitrary web script or HTML via the msg parameter. NOTE: the EsContacts 1.0 issue is covered in CVE-2008-2037.	2009-07-24	4.3	CVE-2008-6876 XF BID SECUNIA MISC
google -- chrome	Google Chrome 2.x through 2.0.172 allows remote attackers to cause a denial of service (application crash) via a long Unicode string argument to the write method, a related issue to CVE-2009-2479.	2009-07-22	5.0	CVE-2009-2578 BUGTRAQ MISC
ibm -- tivoli_identity_manager	Multiple session fixation vulnerabilities in IBM Tivoli Identity Manager (ITIM) 5.0.0.6 allow remote attackers to hijack web sessions via unspecified vectors involving the (1) console and (2) self service interfaces.	2009-07-23	6.8	CVE-2009-2583 VUPEN BID CONFIRM
isc -- dhcp	dhcpd in ISC DHCP 3.0.4 and 3.1.1, when the dhcp-client-identifier and hardware ethernet configuration settings are both used, allows remote attackers to cause a denial of service (daemon crash) via unspecified requests.	2009-07-17	5.0	CVE-2009-1892 BID DEBIAN
kde -- konqueror	KDE Konqueror allows remote attackers to cause a denial of service (memory consumption) via a large integer value for the length property of a Select object, a related issue to CVE-2009-1692.	2009-07-20	4.3	CVE-2009-2537 BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ MILWORM MISC
lullabot -- fivestar_module_for_drupal	Cross-site request forgery (CSRF) vulnerability in the Fivestar module 5.x-1.x before 5.x-1.14 and 6.x-1.x before 6.x-1.14, a module for Drupal, allows remote attackers to hijack the authentication of arbitrary users for requests that cast votes.	2009-07-22	6.8	CVE-2009-2572 VUPEN CONFIRM
marcelo_costa -- fileserver	Directory traversal vulnerability in the Marcelo Costa FileServer component 1.0 for Microsoft Windows Live Messenger and Messenger Plus! Live (MPL) allows remote authenticated users to list arbitrary directories and read arbitrary files via a .. (dot dot) in a pathname.	2009-07-20	6.8	CVE-2009-2544 MILWORM
merlix -- educate_server	Merlix Educate Server allows remote attackers to bypass intended security restrictions and obtain sensitive information via a direct request to (1) config.asp and (2) users.asp.	2009-07-23	5.0	CVE-2008-6870 XF MILWORM
merlix -- educate_server	Merlix Educate Server stores db.mdb under the web root with insufficient access control, which allows remote attackers to obtain unspecified sensitive information via a direct request.	2009-07-23	5.0	CVE-2008-6871 XF OSVDB MILWORM SECUNIA
microsoft -- internet_explorer	Microsoft Internet Explorer 5 through 8 allows remote attackers to cause a denial of service (memory consumption and application crash) via a large integer value for the length property of a Select object, a related issue to CVE-2009-1692.	2009-07-20	4.3	CVE-2009-2536 BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ MILWORM MISC

microsoft -- ie	Microsoft Internet Explorer 6.0.2900.2180 and earlier allows remote attackers to cause a denial of service (CPU and memory consumption) via a long Unicode string argument to the write method, a related issue to CVE-2009-2479.	2009-07-22	5.0	CVE-2009-2576 BUGTRAQ BUGTRAQ BUGTRAQ MISC
mozilla -- firefox mozilla -- seamonkey mozilla -- thunderbird	Mozilla Firefox before 2.0.0.19 and 3.x before 3.0.5, SeaMonkey, and Thunderbird allow remote attackers to cause a denial of service (memory consumption and application crash) via a large integer value for the length property of a Select object, a related issue to CVE-2009-1692.	2009-07-20	5.0	CVE-2009-2535 MISC BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ MILWoRM MISC
mozilla -- firefox	Mozilla Firefox before 3.0.12 does not always use XPCCrossOriginWrapper when required during object construction, which allows remote attackers to bypass the Same Origin Policy and conduct cross-site scripting (XSS) attacks via a crafted document, related to a "cross origin wrapper bypass."	2009-07-22	4.3	CVE-2009-2472 VUPEN BID CONFIRM
netscape -- navigator	Netscape 6 and 8 allows remote attackers to cause a denial of service (memory consumption) via a large integer value for the length property of a Select object, a related issue to CVE-2009-1692.	2009-07-20	4.3	CVE-2009-2542 BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ MILWoRM MISC
olle_johansson -- jobline	SQL injection vulnerability in the search method in jobline.class.php in Jobline (com_jobline) 1.1.2.2, 1.3.1, and possibly earlier versions, a component for Joomla!, allows remote attackers to execute arbitrary SQL commands via the search parameter in a results action to index.php, which invokes the search method from the searchJobPostings function in jobline.php.	2009-07-20	6.8	CVE-2009-2554 XF BID MILWoRM SECUNIA
opera -- opera_browser	Opera, possibly 9.64 and earlier, allows remote attackers to cause a denial of service (memory consumption) via a large integer value for the length property of a Select object, a related issue to CVE-2009-1692.	2009-07-20	4.3	CVE-2009-2540 BUGTRAQ BUGTRAQ BUGTRAQ BUGTRAQ MILWoRM MISC
opera -- opera_browser	Opera 9.52 and earlier allows remote attackers to cause a denial of service (CPU and memory consumption, and application hang) via a long Unicode string argument to the write method, a related issue to CVE-2009-2479.	2009-07-22	5.0	CVE-2009-2577 BUGTRAQ MISC
oramom -- oramom	Oramon Oracle Database Monitoring Tool 2.0.1 stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database containing credentials via a direct request for config/oramom.ini.	2009-07-23	5.0	CVE-2008-6869 XF VUPEN MILWoRM
realnetworks -- helix_server	rmserver in RealNetworks Helix Server and Helix Mobile Server before 13.0.0 allows remote attackers to	2009-07-		CVE-2009-2533 BID

realnetworks -- helix_server_mobile	cause a denial of service (daemon exit) via multiple RTSP SET_PARAMETER requests with empty DataConvertBuffer headers.	2009-07-20	5.0	BUGTRAQ MILWORM MISC CONFIRM
realnetworks -- helix_server realnetworks -- helix_server_mobile	RealNetworks Helix Server and Helix Mobile Server before 13.0.0 allow remote attackers to cause a denial of service (daemon crash) via an RTSP SETUP request that (1) specifies the / URI or (2) lacks a / character in the URI.	2009-07-20	5.0	CVE-2009-2534 BID BUGTRAQ MILWORM MISC CONFIRM
resalecode -- hotscripts_type_php_clone_script	Multiple cross-site scripting (XSS) vulnerabilities in Hotscripts Type PHP Clone Script allow remote attackers to inject arbitrary web script or HTML via the msg parameter to (1) feedback.php, (2) index.php, and (3) lostpassword.php.	2009-07-24	4.3	CVE-2009-2588 XF VUPEN SECUNIA MISC OSVDB OSVDB OSVDB
resalecode -- hutscripts_php_website_script	Multiple cross-site scripting (XSS) vulnerabilities in Hutscripts PHP Website Script allow remote attackers to inject arbitrary web script or HTML via the msg parameter to (1) feedback.php, (2) index.php, and (3) lostpassword.php.	2009-07-24	4.3	CVE-2009-2589 XF VUPEN SECUNIA MISC OSVDB OSVDB OSVDB
scriptsez -- easy_image_downloader	Multiple cross-site scripting (XSS) vulnerabilities in ScriptsEz Easy Image Downloader allow remote attackers to inject arbitrary web script or HTML via the id parameter in a detail action to (1) main.php and possibly (2) demo_page.php.	2009-07-20	4.3	CVE-2009-2551 XF BID SECUNIA MISC OSVDB
supersimple -- super_simple_blog_script	Multiple directory traversal vulnerabilities in comments.php in Super Simple Blog Script 2.5.4 allow remote attackers to overwrite, include, and execute arbitrary local files via the entry parameter.	2009-07-20	6.8	CVE-2009-2552 XF MILWORM SECUNIA
supersimple -- super_simple_blog_script	Multiple SQL injection vulnerabilities in comments.php in Super Simple Blog Script 2.5.4, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via the entry parameter.	2009-07-20	6.8	CVE-2009-2553 XF MILWORM SECUNIA
t-okada -- shiromuku(fs6)diary	Cross-site scripting (XSS) vulnerability in Perl CGI's By Mrs. Shiromuku shiromuku(fs6)DIARY 2.40 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2009-07-21	4.3	CVE-2009-2565 XF CONFIRM SECUNIA JVND JVN
verliadmin -- verliadmin	Multiple cross-site scripting (XSS) vulnerabilities in index.php in VerliAdmin 0.3.7 and 0.3.8 allow remote attackers to inject arbitrary web script or HTML via (1) the URI, (2) the q parameter, (3) the nick parameter,	2009-07-22	4.3	CVE-2009-2571 XF VUPEN BID

	or (4) the nick parameter in a bantest action.			BID MISC
verlihub-project -- verlihub_control_panel	Multiple cross-site scripting (XSS) vulnerabilities in Verlihub Control Panel (VHCP) 1.7e allow remote attackers to inject arbitrary web script or HTML via (1) the nick parameter in a login action to index.php or (2) the URI in a news request to index.html.	2009-07-22	4.3	CVE-2009-2569 VUPEN BID SECUNIA MISC
wireshark -- wireshark	Buffer overflow in the IPMI dissector in Wireshark 1.2.0 allows remote attackers to cause a denial of service (crash) via unspecified vectors related to an array index error. NOTE: some of these details are obtained from third party information.	2009-07-21	5.0	CVE-2009-2559 CONFIRM VUPEN
wireshark -- wireshark	Multiple unspecified vulnerabilities in Wireshark 1.2.0 allow remote attackers to cause a denial of service (crash) via unspecified vectors in the (1) Bluetooth L2CAP, (2) RADIUS, or (3) MIOB dissectors.	2009-07-21	5.0	CVE-2009-2560 CONFIRM
wireshark -- wireshark	Unspecified vulnerability in the sFlow dissector in Wireshark 1.2.0 allows remote attackers to cause a denial of service (CPU and memory consumption) via unspecified vectors.	2009-07-21	5.0	CVE-2009-2561 CONFIRM VUPEN BID
wireshark -- wireshark	Unspecified vulnerability in the AFS dissector in Wireshark 0.9.2 through 1.2.0 allows remote attackers to cause a denial of service (crash) via unknown vectors.	2009-07-21	5.0	CVE-2009-2562 CONFIRM BID

[Back to top](#)

There were no low vulnerabilities recorded this week.

Last updated **July 27, 2009**

 [Print This Document](#)